(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
26. Juli 2001 (26.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/53931 A2

(51) Internationale Patentklassifikation[7]: G06F 9/00

(21) Internationales Aktenzeichen: PCT/DE01/00018

(22) Internationales Anmeldedatum:
5. Januar 2001 (05.01.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
00100954.7 18. Januar 2000 (18.01.2000) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **GAMMEL, Berndt** [DE/DE]; Ludwig-Dill-Weg 3, 81737 München (DE). **KNIFFLER, Oliver** [DE/DE]; Weddigenstr. 1, 81737 München (DE). **SEDLAK, Holger** [DE/DE]; Neumünster 10A, 85658 Egmating (DE).

(74) Anwalt: **EPPING HERMANN & FISCHER**; Postfach 12 10 26, München 80034 (DE).

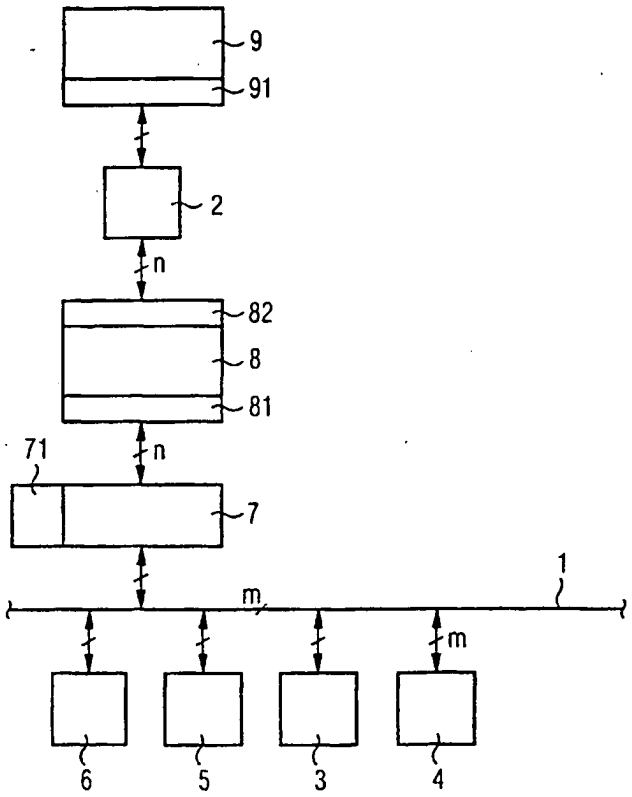
(81) Bestimmungsstaaten *(national)*: BR, CN, IN, JP, KR, MX, RU, UA, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: MICROPROCESSOR SYSTEM AND METHOD FOR OPERATING A MICROPROCESSOR SYSTEM

(54) Bezeichnung: MIKROPROZESSORANORDNUNG UND VERFAHREN ZUM BETREIBEN EINER MIKROPROZESSORANORDNUNG



(57) **Abstract:** A microprocessor system wherein data is temporarily stored in a cache memory (8) or a register bank (9). A respectively allocated cryptographic unit (81, 82; 91) is responsible for encrypting/decrypting the data when the cache memory (8) or register bank is accessed. The code word used therefor is modified when the cache memory (8) or register (9) no longer contains any data which is to be read. This results in increased security with respect to unauthorized access to data and program execution.

(57) **Zusammenfassung:** Bei einer Mikroprozessoranordnung werden Daten temporär in einem Cache-Speicher (8) oder einer Registerbank (9) gespeichert. Eine jeweils zugeordnete kryptographische Einheit (81, 82; 91) sorgt für eine Ver-/Entschlüsselung der Daten bei einem Zugriff auf den Cache-Speicher (8) bzw. die Registerbank (9). Das dabei verwendete Schlüsselwort wird verändert, wenn der Cache-speicher (8) bzw. das Register (9) keine gültigen auszulesenden Daten mehr enthält. Dadurch wird eine erhöhte Sicherheit vor einem Ausspähen von Daten und Programmablauf erhalten.

WO 01/53931 A2

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Mikroprozessoranordnung und Verfahren zum Betreiben einer Mikroprozessoranordnung

Die Erfindung betrifft eine Mikroprozessoranordnung mit einer Verarbeitungseinheit und einem Speicher, der zur Ausführung eines Lese- oder Schreibzugriffs mit der Verarbeitungseinheit gekoppelt ist.

Die Erfindung betrifft außerdem ein Verfahren zum Betreiben einer Mikroprozessoranordnung mit einem solchen Speicher.

Mikroprozessoren benötigen einen Speicher, um dauerhaft oder flüchtig zu verarbeitende Daten oder Programme zu speichern. Bei der Abarbeitung des Programms greift der Mikroprozessor auf den Speicher zu, um aktuell benötigte Programmteile oder Daten zu laden. Mikroprozessoren finden unter anderem Anwendung in sicherheitskritischen Systemen, beispielsweise in Chipkarten. Der Mikroprozessor wird dort unter anderem dazu verwendet, um Datenverkehre zu verschlüsseln oder andere sicherheitskritische Anwendungen für den Chipkarteninhaber abzuwickeln. Dabei sind sicherheitskritische Daten und Programme in den flüchtigen und nichtflüchtigen Speichereinheiten des Mikroprozessors gespeichert. Um ein Ausspähen und Sichtbarmachen dieser Informationen zu verhindern, sind solche Daten verschlüsselt gespeichert. Das Verschlüsselungsverfahren ist relativ aufwendig und erfordert entsprechenden Hardware-Aufwand und Rechenzeit während den Lese- und Schreibzugriffen auf diese Speicher.

Die aktuell von der zentralen Verarbeitungs- und Steuereinheit (CPU) des Mikroprozessors zu verarbeitenden Daten werden daher in weiteren Speichern zwischengespeichert, die wesentlich schneller antworten können. Zum einen ist ein Cache-Speicher vorgesehen, in dem aus den langsameren verschlüsselten Speichern auszulesende oder dorthin zu schreibende Daten

zwischengespeichert werden. Zum anderen sind Register vorgesehen, in denen aktuelle zu verarbeitende Datenwerte oder Betriebseinstellungen zwischengespeichert werden.

Da bei einer Zugriffsanfrage an den Cache-Speicher oder eines der Register die Informationen möglichst schon im nächsten Arbeitstakt zur Verfügung stehen sollen, wird dort eine Verschlüsselung der zwischengespeicherten Information bisher nicht erwogen. Wenn man herkömmliche Verschlüsselungsverfahren für die Verschlüsselung des Inhalts von Cache-Speichern oder Registern anwenden würde, wäre die Antwortzeit zu groß. Daher werden die Daten in Cache-Speichern und den Arbeitsregistern des Prozessors bisher im Klartext zwischengespeichert. Problematisch ist, daß die Daten durch geeignete Meßmethoden ausgespäht werden könnten.

Die Aufgabe der Erfindung besteht darin, eine Mikroprozessoranordnung anzugeben, die eine höhere Sicherheit vor einem Ausspähen abgespeicherter Daten aufweist.

Eine weitere Aufgabe der Erfindung besteht darin, ein Verfahren zum Betreiben einer Mikroprozessoranordnung mit einem Speicher anzugeben.

Betreffend die Anordnung wird diese Aufgabe durch eine Mikroprozessoranordnung gelöst, die umfaßt: eine Verarbeitungseinheit; einen Speicher, der mit der Verarbeitungseinheit zur Ausführung eines Lese- oder Schreibzugriffs gekoppelt ist; eine kryptographische Einheit zur Verschlüsselung und Entschlüsselung von in den Speicher geschriebenen oder gelesenen Datenwerten; Mittel zur Bereitstellung eines veränderbaren Schlüssels, wobei die Mittel derart steuerbar sind, daß der Schlüssel geändert wird, wenn im Speicher keine auszulesenden Datenwerte mehr enthalten sind.

Betreffend das Verfahren wird diese Aufgabe durch ein Verfahren zum Betreiben einer Mikroprozessoranordnung gelöst, die

eine Verarbeitungseinheit und einen Speicher enthält, der mit der Verarbeitungseinheit zur Ausführung eines Lese- oder Schreibzugriffs gekoppelt ist, bei dem während eines Zugriffs auf den Speicher durch die Mikroprozessoranordnung die Datenwerte gemäß einem Schlüssel ver- oder entschlüsselt werden und der Schlüssel geändert wird, wenn keine auszulesenden Daten im Speicher mehr enthalten sind.

Bei einer Mikroprozessoranordnung gemäß der Erfindung ist im Zugangspfad zu einem Speicher, der mit der Verarbeitungseinheit gekoppelt ist, beispielsweise ein Cache-Speicher oder ein Register, im Unterschied zu bekannten Mikroprozessoranordnungen zusätzlich eine kryptographische Einheit eingefügt. Der Schlüssel, unter dessen Verwendung die Ver- bzw. Entschlüsselung betrieben wird, wird verändert. Damit das Ein- und Auslesen in bzw. aus dem Speicher mit dem gleichen Schlüssel ausgeführt werden kann, erfolgt der Wechsel des Schlüssels nur, wenn im Speicher keine auszulesenden Datenwerte mehr enthalten sind. Wegen des wechselnden Schlüssels kann das Verschlüsselungsverfahren selbst relativ einfach sein. Die Daten sind im Speicher nichtflüchtig gespeichert, so daß auch nach dem Abschalten der Versorgungsspannung keine verwertbaren Informationen mehr vorliegen und wiederholte Ausleseversuche keinen Erfolg haben. Während des Betriebs ist die verfügbare Zeit zum Ausspähen des Schlüssels bis zu einem Schlüsselwechsel gering. Insgesamt bietet die Kombination aus veränderbaren Schlüssel mit einem einfachen Verschlüsselungsverfahren ausreichend hohe Sicherheit vor einem Angriff.

Die Erfindung eignet sich besonders in Verbindung mit einem weiteren, langsameren Speicher, in welchem die Daten mit einer harten, aufwendigen Verschlüsselung gespeichert sind. Die Daten werden zur schellen Bereitstellung an die zentrale Verarbeitungseinheit des Prozessors im erfindungsgemäß beschalteten Speicher zwischengepuffert. Die weiteren, hart verschlüsselten Speicher können nichtflüchtige Speicher wie ROMs oder E^2PROMs oder flüchtige RAMs sein. In herkömmlichen Pro-

zessorarchitekturen greift die CPU über einen Bus auf diese Speicher zu. Der Cache-Speicher liegt demgegenüber zwischen Bus und CPU. Bei der Anwendung der Erfindung auf eine Registerbank sind die Register wie herkömmlich direkt an die CPU angeschlossen. Der Cache-Speicher ist dadurch gekennzeichnet, daß bei einer Zugriffsanfrage an einen externen, d.h. nur über den Bus zugänglichen Speicher zuerst überprüft wird, ob ein Datenwert im Cache-Speicher enthalten ist. Ist der Datenwert dort enthalten, wird er aus dem Cache-Speicher und nicht aus dem externen Speicher an den Prozessor ausgegeben. Wenn der nachgefragte Datenwert nicht im Cache-Speicher enthalten ist, wird der Cache-Speicher zuerst mit dem Datenwert und ein geeignetes Umfeld dieses Datenwerts nachgeladen, wobei der angeforderte Datenwert auch an die CPU ausgegeben wird. Der Cache-Speicher enthält hierzu ein Speicherfeld, um das Vorhandensein des angeforderten Datenwerts feststellen zu können. Die Speicherzellen des Speicherzellenfeldes sind statische oder dynamische Speicherzellen. Eine Registerbank ist dadurch gekennzeichnet, daß sie eine Vielzahl von Registern enthält, die von der CPU direkt ansprechbar sind. Die Register stellen beispielsweise Operanden für in der CPU zu verarbeitende logische Verknüpfungen bereit oder Status- und Konfigurationseinstellwerte. Die Registerzellen sind als bistabile Kippstufen oder Flipflops ausgeführt.

Der Schaltungsaufwand für die Verschlüsselung sieht logische Verknüpfungselemente, zweckmäßigerweise Exklusiv-ODER-Gatter, vor, die in die Datenleitungen im Zugriffspfad des Speichers geschaltet sind. Die zu speichernden oder auszulesenden Daten des Speichers werden mit einem Schlüsselwort über die Exklusiv-ODER-Gatter verknüpft. Das Schlüsselwort wird von einem Register bereitgestellt, welches den von Zeit zu Zeit veränderbaren Schlüssel enthält. Die Schlüsselworte werden vorzugsweise zufallsgesteuert erzeugt. Hierzu dient ein Zufallsgenerator, der ausgangsseitig mit dem Schlüsselregister verbunden ist. Der Zufallsgenerator stellt den Schlüssel physikalisch zufällig oder pseudozufällig bereit.

Der Zufallsgenerator wird dann zur Bereitstellung eines neuen Schlüsselworts veranlaßt, wenn im Speicher keine gültigen Daten mehr vorhanden sind. Dies trifft einerseits dann zu, wenn alle in den Speicher eingelesenen Daten bereits wieder ausgelesen sind. Dies trifft andererseits auch dann zu, wenn der Prozessor auf eine andere Anwendung umgeschaltet wird und hierzu neu initialisiert wird. Auf herkömmliche Weise mußte dann der Inhalt des Speichers vollständig gelöscht werden, so daß für die nachfolgende Anwendung keine Daten der vorhergehenden Anwendung mehr verfügbar sind. Bei der Erfindung ist ein Initialisieren des Speichers, indem jede Speicherzelle zurückgesetzt wird, nicht mehr erforderlich. Es genügt vielmehr, nur den Schlüssel zufallsgesteuert zu verändern. Die im Speicher enthaltenen Datenwerte sind dann nicht mehr entschlüsselbar. Ein Rücksetzen jeder einzelnen Speicherzelle ist nicht mehr erforderlich.

Nachfolgend wird die Erfindung anhand des in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert. Einander entsprechende Elemente sind mit gleichen Bezugszeichen versehen. Es zeigen:

Figur 1 ein Blockschaltbild eines Mikroprozessors gemäß der Erfindung und

Figur 2 einen Cache-Speicher, der erfindungsrelevante Details zeigt.

Der Mikroprozessor gemäß Figur 1 umfaßt einen Datenbus 1, über den die verschiedenen Funktionseinheiten des Mikroprozessors miteinander Daten-, Steuerungs- oder Programminformation austauschen. Der Datenbus 1 umfaßt eine Vielzahl von Leitungen zur Übermittlung der Nutz- und Steuerungsinformation. Eine zentrale Verarbeitungseinheit 2 steuert den Programmablauf und führt Berechnungen aus. Daten- und Programminformation sind dauerhaft unveränderbar in einem ROM-Speicher 3 gespeichert oder dauerhaft veränderbar in einem

E^2PROM 4. Flüchtige Daten werden in einem RAM-Speicher 5 abgelegt. Außerdem ist mindestens eine periphere Einheit 6 vorgesehen um Daten von außen zu empfangen oder nach außen abzugeben. Alle Funktionseinheiten sind auf einem einzigen integrierten Halbleiterchip angeordnet. Die Einheiten 2, ..., 6 sind alle an den Bus 1 angeschlossen und tauschen darüber die zu verarbeitende Information aus. Die Zugriffssteuerung auf den Bus wird von einer Bussteuerungseinheit 7 überwacht.

Die in den Speichern 3, 4, 5 abgelegten Daten sind verschlüsselt. Beim Ausgeben der Datenwerte auf den Bus werden die Daten entschlüsselt und als Klartext weitergeleitet. Hierzu dient eine entsprechende Ver- und Entschlüsselungseinheit 71 (MED - Memory En-/Decryption). Beim Einspeichern von Datenwerten in den RAM-Speicher 5 besorgt die Einheit 71 eine entsprechende Verschlüsselung. Da die in den Speichern 3, 4, 5 enthaltenen Daten längerdauernd flüchtig oder nichtflüchtig zur Verfügung stehen ist das von der MED-Einheit 71 abgearbeitete kryptographische Verfahren entsprechend aufwendig. Speicherzugriffe dauern relativ lange. Alternativ zu der zentralen MED-Einheit 71 kann jedem der Speicher 3, 4, 5 direkt eine kryptographische Einheit zugeordnet sein.

Um Datenzugriffe auf die externen Speicher 3, 4, 5 zu beschleunigen, ist ein Cache-Speicher 8 vorgesehen. Der Speicher 8 liegt im Signalpfad zwischen der Bussteuerung 7 und der CPU 2. Im Cache-Speicher 8 werden die aktuell von der CPU 2 angeforderten Daten und ein geeignetes Umfeld dieser Daten zwischengespeichert. Eine Leseanfrage an einen der Speicher 3, 4, 5 wird derart abgearbeitet, daß zuerst im Cache-Speicher 8 überprüft wird, ob dort die angeforderten Daten enthalten sind. Falls nicht, werden die Daten und das entsprechende Umfeld aus den externen Speichern in den Cache nachgeladen. Wenn die angeforderten Daten im Cache 8 enthalten sind, erübrigt sich das Nachladen.

Der Cache-Speicher 8 ist im Ausführungsbeispiel in einen Befehls-Cache-Speicher und einen Daten-Cache-Speicher aufgeteilt. In ersterem werden Befehlsfolgen des gerade abgearbeiteten Programms zwischengespeichert, in letzterem die zugehörigen Daten. Prinzipiell sind auch andere Strukturen für den Cache-Speicher möglich. Der Cache-Speicher kann auch als gemeinsamer Cache für Befehle und Daten ausgelegt sein (Unified Cache). Im Falle einer assoziativen Cache-Speicher-Architektur ist eine solche Einheit wiederum ist in einen Assoziativspeicher für die Adressen aufgeteilt und den zugehörigen Befehls-/Daten-Speicherteil. Durch Abfrage des Assoziativspeichers wird sehr schnell festgestellt, ob das angeforderte Datum im Cache enthalten ist. Wenn das Datum nicht vorhanden ist (sogenannter Cache-Miss) wird eine Anfrage zum Nachladen an den entsprechenden externen Speicher ausgegeben. Entsprechende Vorgänge laufen beim Schreiben eines Datenwerts zurück in das RAM 5 ab.

Beim Nachladen des Cache-Speichers 8 werden die über den Bus 1 empfangenen Informationen in Klartext durch eine kryptographische Einheit 81 verschlüsselt. Bei einem Schreibvorgang werden durch die Einrichtung 81 die im Cache-Speicher 8 verschlüsselt gespeicherten Daten entschlüsselt. Bei der Übermittlung der im Cache-Speicher 8 verschlüsselt gespeicherten Daten an die CPU 2 werden sie durch eine kryptographische Einheit 82 entschlüsselt. Bei einem Schreibvorgang verschlüsselt die Einheit 82 im Cache-Speicher 8 zwischenzuspeichernde Information. Wie weiter unten noch beschrieben, ist der den kryptographischen Einheiten 81, 82 zugeführte Schlüssel identisch und wird zufallsgesteuert verändert, wenn sich im Cache-Speicher 8 keine gültigen auszulesenden Daten mehr befinden.

Operatoren und Statusinformation für die CPU 2 sind in einer Registerbank 9 gespeichert. Auf eines oder mehrere der in der Registerbank 9 angeordneten Register kann die CPU 2 direkt und unmittelbar zugreifen. Dort gespeicherte Daten werden

durch eine kryptographische Einheit 91 beim Zugriff auf eines der Register der Registerbank 9 ver- oder entschlüsselt. Der in den Einheiten 81 und 82 einerseits und der Einheit 91 andererseits verwendete momentane Schlüssel ist zweckmäßiger Weise verschieden.

Die kryptographischen Einheiten sind am Beispiel des Cache-Speichers 8 in Figur 2 im Detail dargestellt. Ein Schlüsselregister 83 enthält den momentan verwendeten Schlüssel. Der Schlüssel wird von einem Zufallsgenerator 84 bereitgestellt, welcher das Schlüsselwort physikalisch echt zufällig oder pseudo-zufällig erzeugt. In die Datensignal- oder Bitleitungen, welche die in den Cache-Speicher 8 eingeschriebene oder davon ausgelesene Information führen sind jeweilige Exklusiv-ODER-Gatter 85a, 85b und 85c geschaltet. Jedes der Exklusiv-ODER-Gatter 85 ist außerdem mit einem Ausgang des Registers 83 verbunden. Die Exklusiv-ODER-Gatter 85 liegen sowohl auf der dem Bus 1 zugewandten als auch auf der der CPU 2 zugewandten Seite des Cache-Speichers 8. Beim Einlesen von Daten in den Cache-Speicher 8 erfolgt aufgrund der Exklusiv-ODER-Verknüpfung der Datenwerte mit dem aus dem Register 83 zugeführten Schlüsselwort eine Verschlüsselung. Beim Auslesen erfolgt durch die gleiche Exklusiv-ODER-Verknüpfung mit dem gleichen Schlüsselwort die komplementäre Entschlüsselung. Solange im Cache-Speicher 8 gültige Daten zum Auslesen gespeichert sind, muß das vom Register 83 bereitgestellte Schlüsselwort unverändert gleich bestehen bleiben. Jeder der n Bitleitungen entspricht ein Bit des Schlüsselworts.

Gemäß der Erfindung wird das Schlüsselwort dann geändert, wenn der Cache-Speicher 8 keine gültigen Daten, d.h. solche Daten, die noch auszulesen sind, enthält. Dann wird der Zufallsgenerator 84 aktiviert, um ein zufallsgesteuert erzeugtes neues Schlüsselwort zu berechnen. Es sind keine gültigen Daten im Speicher 8 mehr enthalten, wenn alle dort zwischengespeicherten Datenwerten wieder ausgelesen sind. Des weiteren ist das Schlüsselwort bei einer Initialisierung des

Cache-Speichers 8, einem sogenannten Cache-Flush, zu verändern. Ein Cache-Flush erfolgt beispielsweise bei einer Änderung des vom Mikroprozessor abgearbeiteten Programms, wenn die Applikation, d.h. der Anwendungsfall, in welchem der Mikroprozessor eingesetzt wird, wechselt. In diesem Fall kann auch auf einen Cache-Flush und ein dadurch bedingtes vollständiges Initialisieren und Rücksetzen sämtlicher Speicherzellen des Cache-Speichers 8 verzichtet werden, da durch ein Wechseln des Schlüsselworts im Register 83 die Daten ohnehin nicht mehr entschlüsselbar sind.

Die kryptographische Einheit 91 ist entsprechend einer der kryptographischen Einheiten im Zugangspfad an den Cache-Speicher 8 im Detail aufgebaut. Deren Schlüsselregister wird dann mit einem neuen Zufallswert geladen, wenn sämtliche Register der Registerbank 9 keine gültigen auszulesenden Daten mehr enthalten oder neu initialisiert werden müssen.

Durch die Erfindung wird eine erhöhte Sicherheit von einem Ausspähen von temporär gespeicherten Daten erhalten, indem die Daten verschlüsselt gespeichert werden und der Schlüssel von Zeit zu Zeit geändert wird. Auch bei mehrfach gleichem Programmablauf sind die gespeicherten Daten aufgrund unterschiedlicher Schlüssel verschieden. Der vom Mikroprozessor während der Abarbeitung des Programms gezogene Strom, insbesondere die Stromspitzen oder Stromtäler, ist unterschiedlich. Dadurch werden Angriffsverfahren, die eine Auswertung des Stromprofils anwenden, erschwert.

Patentansprüche

1. Mikroprozessoranordnung, die umfaßt:
- eine Verarbeitungseinheit (2),
- einen Speicher (8, 9), der mit der Verarbeitungseinheit (2) zur Ausführung eines Lese- oder Schreibzugriffs gekoppelt ist,
- eine kryptographische Einheit (81, 82; 91) zur Verschlüsselung und Entschlüsselung von in den Speicher (8; 9) geschriebenen oder gelesenen Datenwerten,
- Mittel (83) zur Bereitstellung eines veränderbaren Schlüssels, wobei
- die Mittel (83) derart steuerbar sind, daß der Schlüssel geändert wird, wenn im Speicher (8) keine auszulesenden Datenwerte mehr enthalten sind.

2. Mikroprozessoranordnung nach Anspruch 1,
g e k e n n z e i c h n e t d u r c h
einen weiteren Speicher (3, 4, 5), in dem Datenwerte verschlüsselt speicherbar sind, und eine Entschlüsselungseinrichtung (71), durch die die Datenwerte des weiteren Speichers (3, 4, 5) beim Auslesen entschlüsselbar sind.

3. Mikroprozessoranordnung nach Anspruch 1 oder 2,
d a d u r c h g e k e n n z e i c h n e t, daß
der Speicher ein Cache-Speicher (8) ist.

4. Mikroprozessoranordnung nach Anspruch 3,
d a d u r c h g e k e n n z e i c h n e t, daß
der Cache-Speicher (8) eine Zugriffssteuerung enthält, durch die zuerst überprüfbar ist, ob ein Datenwert einer Zugriffsanfrage der Verarbeitungseinheit (2) im Cache-Speicher (8) enthalten sind, so daß dann, wenn die Datenwerte der Zugriffsanfrage im Cache-Speicher (8) enthalten sind, aus dem Cache-Speicher (8) ausgelesen werden.

5. Mikroprozessoranordnung nach 3 oder 4,

d a d u r c h g e k e n n z e i c h n e t, daß
ein Bus (1) zur Abwicklung von Datenverkehr vorgesehen ist, daß der Speicher (8) in den Datenpfad zwischen Bus (1) und Verarbeitungseinheit (2) geschaltet ist und daß der weitere Speicher (3, 4, 5) über den Bus (1) mit der Verarbeitungseinheit (2) verbunden ist.

6. Mikroprozessoranordnung nach Anspruch 1 oder 2,
d a d u r c h g e k e n n z e i c h n e t, daß
der Speicher ein Register (9) ist, das Registerzellen umfaßt, die als bistabile Kippstufen ausgeführt sind.

7. Mikroprozessoranordnung nach einem der Ansprüche 1 bis 6,
d a d u r c h g e k e n n z e i c h n e t, daß
die Mittel zur Bereitstellung des veränderbaren Schlüssels ein Register (83) umfassen und daß die Registerausgänge über logische Verknüpfungselemente (85a, 85b, 85c) mit den Leitungen gekoppelt sind, über die auf Speicherzellen im Speicher (8) zugreifbar ist.

8. Mikroprozessoranordnung nach Anspruch 7,
g e k e n n z e i c h n e t d u r c h
einen Zufallsgenerator (84), der mit dem Register (83) zur Einspeisung des Schlüssels gekoppelt ist.

9. Mikroprozessoranordnung nach Anspruch 8,
d a d u r c h g e k e n n z e i c h n e t, daß
das Register (83) aus dem Zufallsgenerator (84) dann ladbar ist, wenn der Mikroprozessor zur Abarbeitung einer anderen Anwendung initialisiert wird.

10. Verfahren zum Betreiben einer Mikroprozessoranordnung, die eine Verarbeitungseinheit (2) und einen Speicher (8; 9) enthält, der mit der Verarbeitungseinheit zur Ausführung eines Lese- oder Schreibzugriffs gekoppelt ist, bei dem während eines Zugriffs auf den Speicher (8; 9) durch die Mikroprozessoranordnung die Datenwerte gemäß einem Schlüssel ver- oder

entschlüsselt werden und der Schlüssel geändert wird, wenn keine auszulesenden Daten im Speicher (8; 9) mehr enthalten sind.

11. Verfahren zum Betreiben einer Mikroprozessoranordnung nach Anspruch 10,
d a d u r c h g e k e n n z e i c h n e t, daß
der Schlüssel zufallsgesteuert geändert wird.

12. Verfahren zum Betreiben einer Mikroprozessoranordnung nach Anspruch 10 oder 11,
d a d u r c h g e k e n n z e i c h n e t, daß
der Schlüssel geändert wird, wenn der Speicher (8; 9) vollständig ausgelesen ist.

13. Verfahren zum Betreiben einer Mikroprozessoranordnung nach Anspruch 10 oder 11,
d a d u r c h g e k e n n z e i c h n e t, daß
der Schlüssel geändert wird, wenn das Programm, welches von der Mikroprozessoranordnung verarbeitet wird, gewechselt wird.

FIG 1

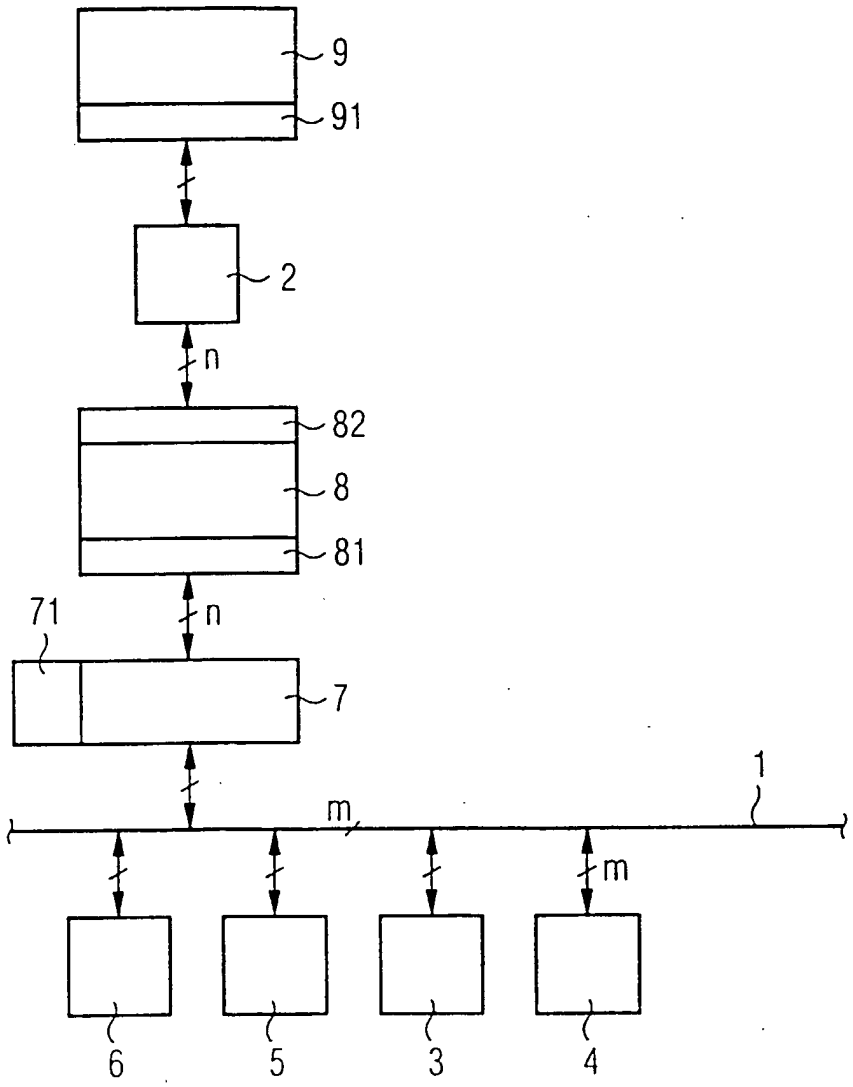


FIG 2